L'accesso ai servizi erogati in rete dagli Enti locali

Alessandro Osnaghi

1 La carta di identità elettronica e l'accesso in internet ai servizi

La **carta di identità elettronica** (CIE) è stata introdotta nel 2000 come **strumento sicuro di identificazione personale per fini di pubblica sicurezza**, in sostituzione dell'attuale documento cartaceo.

La tecnologia molto innovativa allora adottata, consentiva dal punto di vista tecnico di utilizzarla anche per l'autenticazione informatica e il comma 2 dell'Art. 38[1] del DPR. 28 dicembre 2000, n. 445 ***"Testo unico … in materia di documentazione amministrativa"*** ne aveva abilitato l'uso anche per **presentare istanze e dichiarazioni** per via telematica alla pubblica amministrazione, in alternativa all'uso di una **carta di firma digitale.** Una norma specifica si rendeva necessaria proprio perché la **carta d'identità elettronica** non rispondeva ai requisiti tecnici e normativi fissati per le carte di firma digitale e quindi **non poteva essere utilizzata per apporre una firma digitale**. Questa ulteriore funzionalità era infatti stata prevista solo come opzionale e a richiesta del titolare.

Operando nelle due modalità ammesse dall'Art. 38 si ottengono, rispetto al documento informatico generato, risultati molto diversi. Con la **carta di firma digitale** si può generare, anche in modalità fuori linea, un **documento informatico sottoscritto digitalmente**, giuridicamente valido in sé, che successivamente può essere inviato per via telematica alla amministrazione. Con la **carta d'identità elettronica**, se non prevede l'estensione di firma digitale, si può **autenticare l'utente**, ma non si dispone dello strumento tecnico per attribuire al documento informatico, generato durante la sessione interattiva, le proprietà intrinseche di **imputabilità, di integrità e di non ripudio,** che caratterizzano la firma digitale e che consentono di dare pieno valore legale alla istanza.

L'Art. 38, nel considerare giuridicamente valida un'istanza compilata durante una sessione di lavoro in linea, se **autenticata tramite CIE,** introduce una possibilità normativa che appare ragionevole, ma che presenta implicazioni non banali per ottenere, anche in questo

---

[1] *Articolo 38 (L-R) DPR n. 445/2000:* ***Modalità di invio e sottoscrizione delle istanze***

1. *Tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica. (L)*
2. *Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale o quando il sottoscrittore è* ***identificato dal sistema informatico con l'uso della carta d'identità elettronica****.(R).*

modo, un documento informatico che sia almeno **imputabile** all'utente in modo intrinseco e persistente, al fine di consentirne una gestione omogenea con la gestione adottata per i **documenti sottoscritti digitalmente**. Uscendo dalla metafora informatica, è come se si fosse stabilito ope legis che un testo in forma scritta privo di firma autografa deve essere considerato equivalente ad un documento sottoscritto perché è accompagnato dalla esibizione della carta di identità di chi se ne dichiara l'autore.

Nella passata legislatura, sempre con riferimento alla sola presentazione di istanze e comunicazioni, l'Art. 38 del DPR 445/2000 veniva modificato dal Dlgs 23 gennaio 2002, n. 10, con l'introduzione della **carta nazionale dei servizi** (CNS), dispositivo di natura allora imprecisata, che ai fini dell'accesso poteva sostituire le funzioni della CIE, e si poteva allora successivamente assistere ad una pubblica competizione tra membri del governo che promuovevano ciascuno una propria carta, invece di operare congiuntamente per accelerare la distribuzione della CIE. Il comma 2 Art. 38, originariamente di rango regolamentare, veniva inoltre **innalzato a rango di norma primaria** e si rafforzava così la convinzione generale, priva di precedenti nella normativa antecedente, che per accedere ai servizi fosse necessaria comunque una smart card.

Da questa convinzione deriva, evidentemente, la discussa formulazione dell'Art. 64[2] del DLgs. 7 marzo 2005, n. 82 "***Codice della amministrazione digitale"*** che **rende obbligatorio**, dopo il 31 dicembre 2007, l'uso di una CIE o CNS per autenticarsi a tutti i servizi erogati in internet della pubblica amministrazione, senza alcun riferimento alle effettive **esigenze di sicurezza e di imputabilità** richieste da ogni specifico servizio.

---

*2 Art. 64. **Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni**.*

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. E' prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.

È necessario osservare che mentre l'Art. 64 ha reso obbligatorio per qualsiasi servizio l'uso della CIE, rispetto alla normativa antecedente, il comma 1, lettera b dell'Art. 65[3] ne ha invece **depotenziato l'uso** proprio per i **servizi di presentazione di istanze e comunicazioni**, perché lo consente solo ***"nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente"***. Non possono sfuggire l'incoerenza di questa previsione, probabilmente dettata da una malinteso desiderio di rispettare l'autonomia delle amministrazioni locali, e gli **effetti irrazionali che ne possono derivare**. Ad ogni piccolo, medio o grande comune è quindi consentito limitare la possibilità di uso della CIE per la presentazione di specifiche istanze, anche se è difficile comprendere in base a quali criteri gli Enti locali potrebbero stabilire condizioni di accesso diverse tra loro per le presentazione delle medesime istanze.

La CIE ha finora incontrato difficoltà di distribuzione - sui cui motivi non è qui rilevante soffermarsi - e **bene ha fatto il governo attuale ad attivarsi per rimuovere gli ostacoli e per completarne in tempi brevi la diffusione**, soprattutto in considerazione degli accresciuti rischi per la pubblica sicurezza, che sono stati resi evidenti dopo il settembre 2001 e che sono tali da indurre anche un paese notoriamente sensibile alle tematiche della identificazione personale, come è il Regno Unito, ad approvare recentemente una legge (Identity Cards Act 2006) che istituisce l'anagrafe centralizzata della popolazione e la carta d'identità, in cui tuttavia non si fa alcuna menzione di un suo possibile uso anche per l'accesso telematico.

Non risulta che altri paesi abbiano compiuto il percorso giuridico, che ha compiuto l'Italia con l'Art. 64 del Codice della amministrazione digitale, ed abbiano trasformato un documento di identificazione personale, che oggi non può che essere elettronico, in uno strumento da **usare obbligatoriamente per l'acceso a tutti i servizi erogati in internet dalla pubblica amministrazione**. Allo stato dell'arte delle tecnologie per la sicurezza all'accesso, e nella attuale realtà del mercato ICT, **questo passaggio non appare razionale, utile e neppure pratico**. Se può avere un senso obbligare le amministrazioni ad accettare sempre e comunque la CIE, nel caso un utente sia in grado di usarla, una prescrizione che ne impone l'uso agli utenti per accedere a qualsiasi servizio, che richieda autenticazione, non

---

*3 Art. 65. **Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.***

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;

b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

appare allo stato dell'arte motivata. Anche nel Programma elettorale dell'Unione, del resto, la CIE viene descritta come lo **strumento privilegiato** per l'accesso ai servizi e quindi evidentemente **non l'unico**.

Ben venga l'accelerazione che il governo ha recentemente impresso alla diffusione della CIE, purché questa azione non offuschi l'esigenza delle necessarie correzioni che si dovranno apportare alla legge attualmente in vigore per introdurre **norme primarie più razionali e di validità generale**, lasciando eventualmente alla normativa secondaria, come era nella 445/2000, la regolamentazione di una materia così strettamente legata alle evoluzioni tecnologiche. Le correzioni da apportare all'Art. 64 del Codice non dovranno quindi limitarsi a **prorogare il termine** in cui scatta l'obbligo di uso della CIE – che, permanendo, determinerebbe la conseguente cessazione della erogazione dei servizi a tutti coloro che non avranno la carta o non saranno attrezzati per utilizzarla - ma soprattutto dovranno **introdurre le necessarie aperture all'utilizzo altri strumenti**, dai più convenzionali come UserID, Password e PIN, alle tecnologie che consentono ad esempio il riconoscimento delle caratteristiche biometriche (impronta digitale o impronta vocale) e che sono già oggi in grado di sostituire le smart card per il controllo degli accessi effettuati in internet.

Infatti mentre l'utilizzo delle smart card per la firma digitale non presenta particolari difficoltà pratiche, l'utilizzo delle smart card per l'autenticazione in rete basata sugli standard internet presenta difficoltà di natura tecnica che non possono essere trascurati e che è necessario chiarire.

L'accesso dei cittadini ai servizi erogati in rete dalle amministrazioni avviene tipicamente utilizzando **stazioni di lavoro private o domestiche** costituite da ***personal computer***, cioè da prodotti commerciali che sono oggi considerati dal mercato come **commodities** e che per connettersi, tramite un fornitore di servizi internet, al sito che eroga il servizio (**il web server** della amministrazione**)** utilizzano un'applicazione standard (**il browser**). Questo modello architetturale si è affermato perché il modello client-server classico che implica la presenza sulla stazione di lavoro dell'utente di **software applicativo specifico del servizio richiesto non è praticabile** dal punto di vista gestionale, anche se non è impossibile da realizzare dal punto di vista tecnico.

Le amministrazioni possono offrire servizi anche attraverso ***public computer*** utilizzando **stazioni di lavoro dedicate** (con varie denominazioni: totem, chioschi o ATM, ecc.) che, pur accessibili in luoghi pubblici, sono supportate direttamente dall'ente e per questo motivo possono ospitare applicazioni che sono specifiche dei servizi erogati. Quando le **smart card**

ospitano dati specifici del servizio **si prestano bene** all'utilizzo **nelle stazioni di lavoro pubbliche** gestite direttamente da una organizzazione, ma **non si prestano bene** all'utilizzo **nelle stazioni di lavoro private** dei cittadini che si connettono da casa in internet ai siti delle amministrazioni.

Nonostante questo dispositivo abbia un costo ininfluente sul costo complessivo di un personal computer i produttori mondiali non forniscono normalmente un lettore di smart card come dispositivo integrato nelle configurazioni standard commerciali (come ad esempio fanno per il lettore di CD o il modem) e anche se ciò sarebbe auspicabile in un paese in cui la legge impone l'uso di smart card (CIE o CNS) per accedere a qualsiasi servizio pubblico. Se le configurazioni dei PC commercializzate sul mercato italiano non prevedono un lettore integrato, tutti i cittadini saranno costretti ad acquistarlo ed installarlo come una periferica aggiuntiva non gestita automaticamente dal software di sistema.

È di tutta evidenza che **l'industria mondiale non intende promuovere le smart-card** come dispositivo privilegiato e standard di accesso, ma che invece presumibilmente doterà a breve i PC di altri dispositivi integrati di autenticazione: ad esempio di un sensore di impronta digitale. Se quindi l'uso di CIE o CNS resterà obbligatorio, sarebbe necessaria una **azione coordinata tra governo e operatori sul mercato italiano** per ottenere, almeno nella versione commercializzata in Italia, la **fornitura di personal computer predisposti all'uso delle smart card previste dalla legge.**

Non è questa tuttavia la difficoltà principale per l'utente, perché non è sufficiente installare un lettore per poter utilizzare una carta. Le smart card, che contengono dati relativi a singoli servizi, richiedono di **installare nella stazione di lavoro dell'utente anche software specifico del servizio**. Per l'utente questa esigenza rappresenta una difficoltà pratica spesso insuperabile e tale da scoraggiare l'uso dei servizi e costituisce per le amministrazioni, in particolare per gli enti locali medi e piccoli, un onere gestionale difficilmente sostenibile. Per questa ragione solo nelle **smart card destinate all'uso in stazioni di lavoro gestite** è possibile memorizzare informazioni necessarie all'erogazione del servizio, altrimenti le informazioni dovranno essere conservate nei sistemi informativi delle amministrazioni e reperite tramite rete. Se poi le carte sono multi-servizio, come sono la CIE o le varie CNS e contengono dati relativi a servizi erogati da amministrazioni diverse, la complessità gestionale diventa davvero impraticabile.

In conclusione le smart card che contengono **dati relativi ai servizi** sono destinate ad essere usate **solo su stazioni di lavoro accessibili al pubblico** gestite o attrezzate dalle

singole amministrazioni, mentre le smart card da utilizzare sulle **stazioni di lavoro private** per l'accesso via internet **non devono "contenere servizi"** (stereotipo linguistico improprio, ma usato frequentemente) e non devono essere usate come sostituti elettronici dei certificati cartacei, mediante i quali l'utente trasporta informazioni da una amministrazione ad un'altra. Queste carte devono memorizzare solo informazioni, non modificabili e standard, per identificare il titolare (ad esempio un certificato X509 di autenticazione o di non ripudio) e potranno essere utilizzate solo per l'**autenticazione informatica** o per la **firma digitale.**

Tuttavia, le numerose tipologie di carte circolanti in Italia, anche se conformi alla normativa, non hanno ancora raggiunto, neppure per la semplice funzione di autenticazione, un livello di standardizzazione sufficiente a rendere il **software della stazione di lavoro indipendente** dal particolare tipo di smart card. In questo quadro diventa estremamente oneroso, se non velleitario, assicurare l'interoperabilità sulla stessa stazione di lavoro di smart card con diverse funzioni e fornite da soggetti diversi, come ad esempio la CIE o le CNS ed i vari tipi di carte di firma digitale, anche se si tratta di requisito essenziale per gli utenti.

La difficoltà non è di natura tecnica ed il problema non è insolubile. Da un lato sarebbe necessario, almeno per le esigenze della pubblica amministrazione (ma potrebbe servire anche per servizi erogati da soggetti privati), completare un processo di standardizzazione che non è stato finora gestito sapientemente dagli organismi preposti (prima AIPA poi CNIPA), dall'altro bisognerebbe raggiungere accordi con i distributori di PC sul mercato italiano perché distribuiscano e supportino versioni predisposte per la gestione delle principali carte legalmente valide che circolano in Italia, inclusa la CIE.

È sicuramente apprezzabile l'azione di accelerazione promossa dal governo per la distribuzione della carta di identità elettronica, che mantiene tutta la sua validità come strumento per l'identificazione personale ai fini di pubblica sicurezza e che è sicuramente utilizzabile anche per l'accesso a servizi erogati attraverso **sportelli automatici o postazioni attrezzate** accessibili al pubblico, ma è tuttavia necessario che il legislatore prenda atto che **lo strumento smart card non è di facile e pratico utilizzo per autenticarsi sulle stazioni di lavoro private** da cui i cittadini accedono via internet ai servizi delle amministrazioni e che provveda con urgenza a **modificare la normativa vigente**, che altrimenti diventerà un impedimento alla erogazione dei servizi.

Per non **scoraggiare i cittadini o impedire loro** di accedere ai servizi della pubblica amministrazione per via telematica, è necessario introdurre anche **strumenti convenzionali**

di autenticazione che risultino di "costo" minimo per gli utenti e per le amministrazioni, e utilizzabili anche per accedere a servizi per i quali si renda necessario **l'accertamento dell'identità** personale del richiedente.

Si tratta di un'esigenza molto sentita soprattutto dalle amministrazioni locali e questo documento discute le condizioni e propone soluzioni per assicurare un sufficiente livello di sicurezza all'accesso dei servizi degli Enti locali utilizzando **credenziali**[4] di tipo convenzionale basate su UserID, Password e PIN.

2 Amministrazioni centrali e Enti locali

Le amministrazioni e gli enti centrali (Agenzia delle Entrate, INPS, ecc.) distribuiscono da tempo credenziali di tipo convenzionale (basate su UserID, Password e/o PIN) ai cittadini che si registrano nei loro siti per ottenere l'abilitazione all'accesso telematico ai servizi. Le amministrazioni centrali non erogano servizi a chi non è già censito nelle loro basi dati istituzionali - quindi a chi non è già noto all'amministrazione - e possono mettere in atto particolari accorgimenti per assicurare che la componente segreta delle credenziali sia consegnata con ragionevole sicurezza solo al titolare, chiunque sia il soggetto che provvede materialmente alla registrazione per via telematica.

In particolare l'Agenzia delle entrate rilascia gratuitamente previa registrazione telematica, ad ogni cittadino credenziali convenzionali (UserID = Codice Fiscale, Password e PIN) ed invia la componente segreta - il PIN - in busta cieca all'indirizzo fiscale del titolare. L'accorgimento utilizzato per consentire il sicuro riferimento al titolare delle credenziali fiscali è quello di richiedere, in fase di registrazione, alcune informazioni di natura fiscale variabili nel tempo, che solo il titolare, o un suo fiduciario, può ragionevolmente conoscere (ad esempio il reddito dichiarato negli anni precedenti). È così possibile assicurare la consegna sicura delle credenziali al titolare identificato con il codice fiscale in base al suo domicilio fiscale noto all'amministrazione.

Le credenziali fornite dell'Agenzia delle entrate sono utilizzate per accedere alle informazioni che riguardano la posizione fiscale del titolare e anche per sottoscrivere digitalmente la dichiarazione dei redditi, in deroga alla disciplina generale sulla firma digitale e sul documento informatico. In proposito è interessante notare che il comma 3, Art. 64 del DLgs. 7 marzo 2005, n. 82, ***Codice della amministrazione digitale***, prevede che la disciplina

---

4 Le credenziali sono informazioni associate ad un profilo di utenza, mantenuto dal sistema informativo, che l'utente presenta alla procedura di autenticazione informatica del sistema per ottenere l'accesso a dati e servizi compatibili con il profilo, erogati dal sistema stesso o anche da un altro sistema a lui connesso in un contesto di interoperabilità.

riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali resti in vigore anche oltre il termine del 31 dicembre 2007, introducendo il discutibile principio che le amministrazioni non sono tutte uguali e che anzi, proprio all'amministrazione che ha maggiori capacità di progettualità informatica si rende più facile l'adeguamento alla normativa.

Gli Enti locali si trovano in condizioni diverse rispetto alle amministrazioni centrali, in quanto erogano servizi anche a soggetti non residenti, che non sono censiti nelle basi dati demografiche e non sono in condizioni di assicurare con ragionevole certezza la consegna della componente segreta delle credenziali al soggetto titolare, sulla base di informazioni già in loro possesso. Se non introducono modalità di riconoscimento personale non potranno assicurare che l'accesso ai servizi è **consentito solo a chi ne ha diritto** e tutelare adeguatamente la privacy dei cittadini.

La gran parte dei servizi erogati dagli Enti locali appartiene alla tipologia regolamentata dall'Art. 65 del Codice della **presentazione di istanze e di comunicazioni**. Si tratta di servizi che sono tipicamente utilizzati da professionisti o intermediari, non necessariamente residenti, la cui identità personale può essere considerata irrilevante per l'accesso (infatti piuttosto che autenticarsi al sistema devono in realtà sottoscrivere le istanze presentate) e dei quali è invece rilevante verificare, quando sono necessari per l'accesso al servizio, la qualifica professionale posseduta o il ruolo e anche il possesso delle deleghe ricevute dal soggetto per conto del quale operano. Questa categoria di utenti - si tratta in effetti di un'utenza business - è perfettamente in grado di procurarsi ed utilizzare senza problemi le carte di firma digitale e utilizzarle anche come strumenti di autenticazione ed in molti casi già le usano.

Per i servizi di natura personale destinati ai cittadini che gli Enti locali sono oggi in grado di erogare per via telematica è invece necessario, in attesa di una disponibilità generalizzata della carta d'identità elettronica, evitare discriminazioni ed è quindi urgente individuare, come prevede il comma 2, Art. 64 del Codice della amministrazione digitale, altre modalità **possibilmente uniformi per la distribuzione di credenziali di tipo convenzionale**, che consentano un accesso sicuro.

3 Le problematiche generali dell'accesso ai servizi in rete

L'erogazione in rete di servizi attraverso il proprio sito internet presuppone da parte dell'ente erogatore l'organizzazione e la conduzione di attività di ***provisioning*** di tipo informatico, amministrativo e logistico, che sono connesse alla procedura di **registrazione**

dell'utente con il duplice scopo di fornirgli le **credenziali** da presentare per ottenere l'**autenticazione** per l'accesso ai servizi e di raccogliere le informazioni utili per creare presso il sistema informativo di front-end dell'ente il **profilo dell'utente** che è necessario per intrattenere con lui un **rapporto personalizzato**.

L'esigenza di **registrare gli utenti e di autenticarli** è quindi di natura tecnica e gestionale e può prescindere **dalla tipologia di servizi che vengono erogati** e dai loro requisiti di sicurezza, siano essi servizi erogati da soggetti privati o da pubbliche amministrazioni.

Registrarsi ad un sito internet è oggi una pratica di diffusa e di comune esperienza e comporta l'attivazione di una procedura informatica attraverso la quale l'utente fornisce sia le informazioni necessarie alla creazione del suo profilo - ad esempio indicando un numero di cellulare o un indirizzo di posta elettronica per poter ricevere comunicazioni relative alle richieste di servizio - sia, quando necessario, le informazioni utili alla sua identificazione personale. Attraverso la procedura di registrazione un **utente potenziale** diventa un **utente in atto** noto al sistema informativo di front-end dell'ente e abilitato ad interagire col sistema per accedere ai servizi di back-end per cui è autorizzato[5].

La procedura di registrazione oltre alla creazione del profilo - che è un procedimento puramente informatico - comporta la gestione di attività organizzative, amministrative e logistiche per la generazione e la consegna sicura della parte segreta delle credenziali che l'utente dovrà utilizzare per accedere ai servizi del sito. Le attività di ***provisioning*** comportano **costi significativi**, in gran parte indipendenti dal tipo di credenziali fornite, ed è quindi importante individuare soluzioni che possano essere realizzate a costi minimi per le amministrazioni e per i cittadini, soprattutto se le credenziali potranno essere utilizzate solo fino al 31 dicembre 2007, come attualmente previsto dal comma 3, del già citato Art. 64 del Codice.

Un utente potrà accedere a **servizi personalizzati** solo se è registrato e per ottenere l'accesso dovrà fornire le proprie credenziali ad una procedura informatica di **autenticazione**. Tuttavia l'autenticazione di un utente registrato comporta solamente la verifica della validità delle credenziali e non comporta necessariamente l'**accertamento della sua identità personale**, che invece dipende esclusivamente dalla procedura di registrazione

---

5 In questo documento ci si riferisce sempre ad un modello architetturale del sistema informativo che mantiene una distinzione logica (ma eventualmente anche fisica e gestionale) tra il sistema di front-end e il sistema di back-end di un ente. Il sistema di front-end svolge esclusivamente la funzione di supportare l'utente nella compilazione delle richieste di servizio e nel loro invio al sistema di back-end e sostituisce quindi le funzioni di front-office dell' Ente.

le cui modalità determinano se le **credenziali** possono essere considerate **imputabili**, cioè se sono **associate con certezza all'identità personale del soggetto titolare**.

A prescindere dalla proprietà di imputabilità, le credenziali possiedono, in funzione della tecnologia utilizzata, gradi diversi di **sicurezza** rispetto al rischio di **furto della identità**, cioè alla possibilità di uso improprio da parte di un soggetto che non è il titolare. L'informazione segreta associata alle credenziali può essere "posseduta" in varie forme: nella forma di ***una cosa che so*** (credenziali convenzionali UserID, Password e PIN), nella forma di ***una cosa che ho e una cosa che so*** (credenziali basate su smart-card e PIN), oppure nella forma di ***una cosa che sono ed una cosa che so*** (credenziali basate su dati biometrici e PIN o UserID).

Per decidere quale tipo di credenziali utilizzare in fase di autenticazione diventa allora necessario **caratterizzare i servizi**. Dovrebbero essere identificati i servizi non personalizzati, tipicamente di carattere informativo, che possono essere erogati anche ad **utenti anonimi** non noti al sistema, cioè non registrati e privi di un profilo utente e di credenziali. Dovrebbero poi essere identificati i servizi che richiedono una personalizzazione dell'interazione per i quali è utile che l'utente si registri ed ottenga credenziali, anche se non imputabili. Dovrebbero infine essere identificati i servizi per i quali è **necessario** che le credenziali siano riferibili con certezza **all'identità personale dell'utente**, in modo che il servizio venga erogato **solo a chi ne ha diritto** e con un livello di sicurezza predefinito.

In conclusione dal punto di vista dell'accertamento della identità personale dell'utente sono possibili tre tipologie di utenza:

Utenza anonima: l'utente **non possiede credenziali** e il sistema **non possiede un profilo** dell'utente. Non vi è necessità di eseguire una procedura di autenticazione informatica perché al sistema non interessa distinguere un utente dall'altro.

Utenza non imputabile: il sistema possiede un profilo dell'utente e l'utente possiede **credenziali non imputabili**. La procedura di autenticazione informatica non consente di accertare l'identità personale di chi presenta le credenziali e quindi il sistema può erogare **servizi personalizzati**, ma **non consentire** l'accesso a servizi per i quali è necessario l'accertamento dell'identità personale.

Utenza imputabile: il sistema possiede un profilo dell'utente e l'utente possiede **credenziali imputabili**. In questo caso la procedura di autenticazione consente di accertare l'identità personale di chi presenta le credenziali e quindi **può consentire** l'accesso a servizi per i quali è necessario il riconoscimento personale.

È necessario notare che purché la registrazione avvenga con precise modalità e la componente segreta venga consegnata con ragionevole certezza ed in modo riservato proprio al soggetto che ne è il titolare, **tutte le tipologie di credenziali possono essere imputabili** e quindi non solo l'uso di una smart-card o di una caratteristica biometrica, ma **anche l'uso di credenziali convenzionali UserID, Password o PIN può consentire l'accertamento dell'identità**. Al contrario credenziali ad alto grado di sicurezza, come ad esempio una smart card, potrebbero risultare non imputabili se il riconoscimento personale del titolare non è avvenuto in modo appropriato e certo.

Volendo affrontare correttamente la tematica dell'erogazione in rete dei servizi delle pubbliche amministrazioni e, particolarmente nel caso degli Enti locali, per garantire un'uniformità di accesso per tutti i cittadini, assicurando che gli stessi servizi erogati da enti diversi rispondano agli stessi criteri di imputabilità e di sicurezza, sarebbe importante compilare a livello nazionale una **tassonomia dei servizi** in base all'esigenza di accertamento dell'identità personale e codificarne il **grado di sicurezza** intrinseca richiesto. Tuttavia, come sempre nel caso della sicurezza, sarà opportuno anche confrontarsi con i costi complessivi delle soluzioni e con una analisi dei rischi in relazione ai beni materiali ed immateriali che è necessario proteggere in base alla normativa sulla tutela della privacy.

Il comma 1, Art. 64: *"Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni"* del Codice della amministrazione digitale ha invece ignorato l'esigenza di una classificazione dei servizi e ha imposto l'uso della Carta d'Identità Elettronica - cioè del dispositivo di autenticazione destinato a fornire la massima garanzia di imputabilità e sicurezza - per "***tutti i servizi che richiedono l'autenticazione informatica***" quindi **anche per i servizi** che, pur richiedendo l'autenticazione informatica, **non hanno necessità di accertare l'identità personale del richiedente**. Questa formulazione, a dir poco infelice, produrrà risultati paradossali. Ad esempio non si può escludere che sia opportuno autenticarsi per prenotare via internet un campo da tennis comunale - si tratta pur sempre di un servizio della pubblica amministrazione - ma sembra paradossale che dopo il 31 dicembre 2007 si possa accedere a questo servizio solo utilizzando la Carta d'Identità Elettronica, come prescrive il comma 3 dell'Art. 64.

Oggi le amministrazioni locali sono pronte ad erogare in rete ai cittadini e alle imprese numerosi servizi, ma sono state lasciate sole dal comma 2 dell'Art. 64 nella individuazione delle soluzioni per l'accesso. È necessario dare una **risposta uniforme** a questo problema per

evitare che, a causa della scarsa familiarità degli enti locali con queste tematiche, vengano adottate soluzioni diverse tra loro e poco sicure.

4 Le modalità di registrazione per fornire credenziali imputabili

Le modalità tecnico-organizzative con cui si svolge la **procedura di registrazione** determinano l'**imputabilità** delle credenziali erogate, cioè se sono associabili con certezza all'**identità personale del titolare.**

Per ottenere **credenziali imputabili** l'utente deve presentare una richiesta all'Ente erogatore dei servizi e compilare e sottoscrivere un **modulo di registrazione** con cui fornisce le **informazioni necessarie alla creazione del suo profilo** nel sistema informativo di front-end dell'Ente. Le informazioni che devono essere fornite sono di due tipi:

1. **Informazioni di identità,** che comprendono il Codice Fiscale ed eventualmente le informazioni di identificazione personale in chiaro (cognome, nome, data e luogo di nascita e sesso), peraltro già contenute in forma codificata nel Codice Fiscale;
2. **Informazioni di servizio** che comprendono alcune informazioni necessarie per gestire l'interazione con l'utente, sia telematica che di altro tipo, in relazione ai servizi richiesti a prescindere dalla sua identità personale. (Ad esempio: una casella di posta elettronica; un indirizzo postale o di domicilio; un numero di telefono ecc.). Eventualmente si potranno richiedere altre informazioni utili ai fini della erogazione dei servizi che non fanno già parte delle informazioni che sono associate al soggetto nelle basi dati istituzionali della amministrazione.

Per assicurare l'imputabilità delle credenziali le **informazioni di identità** fornite nel modulo di registrazione devono essere accertate richiedendo l'esibizione un documento di identità valido, mentre le **informazioni di servizio** sono accettate in base alla dichiarazione dell'interessato.

La **certificazione delle informazioni di identità** può avvenire secondo tre modalità:

1. Il **riconoscimento a vista** del soggetto effettuato da un addetto incaricato dall'Ente mediante esibizione di un documento di identità valido.

2. In base **all'Art. 45 del DPR n. 445, 28 dicembre 2000**[6] mediante invio via fax o posta del modulo di registrazione sottoscritto, accompagnato dalla copia fotostatica di un documento di identità valido.

3. **Per via telematica** tramite compilazione sul sito dell'ente ed invio del modulo di registrazione da parte di un utente, che si è autenticato al servizio di registrazione utilizzando la CIE o una CNS.

L'accertamento che le informazioni di identità sono corrette e attribuibili al titolare è quindi in ogni caso basato su varie forme di **esibizione di un documento di identità valido** (esibizione diretta, in fotocopia o per via telematica).

Sia nel caso di credenziali basate su smart-card e PIN, sia nel caso di credenziali convenzionali basate su UserID, Password e PIN, il servizio di registrazione, che genera e consegna le credenziali dell'ente, deve garantire che il **segreto sia consegnato solo nelle mani del titolare** (è il caso di una smart-card), **oppure nelle mani del titolare e di una parte terza** di cui l'utente e l'amministrazione si fidano (è il caso di credenziali convenzionali tipo Password e PIN).

Nel caso di credenziali convenzionali è poi fondamentale per la sicurezza che il servizio di autenticazione, a cui l'utente comunica il proprio segreto, sia realizzato in modo tale da garantire che esso non venga reso noto ad altri sistemi informativi dell'ente. Questa condizione implica l'affidamento di questo servizio ad una **parte fidata** che trasmette al sistema informativo dell'ente solo **asserzioni di identità**, che corrispondono alla sola dichiarazione che le credenziali presentate sono valide. Se queste condizioni sono soddisfatte anche **credenziali convenzionali** basate su UserID, Password e PIN **possono essere considerate imputabili**.

---

*6 Art. 45 (L-R**) Documentazione mediante esibizione***

1. *I dati relativi a cognome, nome, luogo e data di nascita, la cittadinanza, lo stato civile e la residenza attestati in documenti di identità o di riconoscimento in corso di validità, possono essere comprovati mediante esibizione dei documenti medesimi. È fatto divieto alle amministrazioni pubbliche ed ai gestori o esercenti di pubblici servizi, nel caso in cui all'atto della presentazione dell'istanza sia richiesta l'esibizione di un documento di identità o di riconoscimento, di richiedere certificati attestanti stati o fatti contenuti nel documento esibito. È, comunque, fatta salva per le amministrazioni pubbliche ed i gestori e gli esercenti di pubblici servizi la facoltà di verificare, nel corso del procedimento, la veridicità dei dati contenuti nel documento di identità o di riconoscimento. (L)*
2. *Nei casi in cui l'amministrazione procedente acquisisce informazioni relative a stati, qualità personali e fatti attraverso l'esibizione da parte dell'interessato di un documento di identità o di riconoscimento in corso di validità, la registrazione dei dati avviene attraverso l'acquisizione della copia fotostatica non autenticata del documento stesso. (R)*
3. *Qualora l'interessato sia in possesso di un documento di identità o di riconoscimento non in corso di validità, gli stati, le qualità personali e i fatti in esso contenuti possono essere comprovati mediante esibizione dello stesso, purché l'interessato dichiari, in calce alla fotocopia del documento, che i dati contenuti nel documento non hanno subito variazioni dalla data del rilascio. (R)*

Se le credenziali emesse da una amministrazione in base a regole condivise sono imputabili, non c'è motivo che non possano essere accettate anche per accedere ai servizi di un'altra amministrazione. Quando, grazie alla collaborazione tra le amministrazioni, questa possibilità si verifica le credenziali diventano **interoperabili**, cioè fruibili per accedere ai servizi di più amministrazioni. In Italia questa possibilità è facilitata dal fatto che l'identità del cittadino è **codificata nel medesimo e unico modo** presso tutte le pubbliche amministrazioni mediante il **codice fiscale**.

È sicuramente utile individuare le soluzioni praticabili per **ridurre il numero di credenziali** convenzionali da utilizzare per l'acceso a servizi in rete sia pubblici che privati. Infatti oggi un utente medio deve **memorizzare un numero intollerabilmente alto** di UserID, Password e PIN diversi, assegnati da fornitori di servizi privati (Ferrovie, Poste, Banche, ecc.), dalle pubbliche amministrazioni centrali (Agenzia delle Entrate, INPS, ecc.) o per servizi erogati dalle Regioni e Enti locali. Questa situazione oltre a causare un evidente disagio agli utenti riduce grandemente, come noto, il livello di sicurezza inducendo negli utenti comportamenti che facilitano il furto d'identità. È vero che usare la Carta d'Identità elettronica come strumento di autenticazione è un modo per perseguire questo obiettivo - oltre a quello di dotare il cittadino di un documento di identificazione sicuro – ma, come si è cercato di argomentare, non rappresenta purtroppo una soluzione fruibile nella generalità dei casi per l'accesso ad internet.

La riduzione del numero di credenziali che il cittadino deve memorizzare si può ottenere anche utilizzando credenziali di tipo convenzionale imputabili emesse da amministrazioni che adottano **regole comuni** per la realizzazione dei propri **servizi di gestione dell'identità**, oppure che si appoggiano a servizi infrastrutturali erogati da soggetti terzi. Soluzioni di questo tipo **sono già state realizzate** da alcuni Enti locali, che si sono spontaneamente associati per assicurare la interoperabilità delle credenziali convenzionali assegnate da ciascuno di loro. La soluzione generale più auspicabile sarebbe quella di realizzare a livello regionale i servizi di gestione dell'identità per distribuire **credenziali uniche regionali** accettate da tutte le amministrazioni (ed eventualmente anche altri operatori). Tali servizi si potranno federare con quelli delle altre regioni per consentire l'uso delle credenziali di una regione anche per servizi di amministrazioni di altre regioni federate (si tratta di uno degli obiettivi del progetto interregionale ICAR in corso di realizzazione). Si verrebbe così a costituire in forma federata un **sistema nazionale di gestione dell'identità** del tutto indipendente dalle diverse tipologie di credenziali in uso in ogni dato momento, tipologie che sono destinate ad evolvere seguendo i rapidi progressi delle tecniche di identificazione.

5 Una nuova proposta per la registrazione telematica diretta

Il presupposto per la realizzazione di un sistema unico di credenziali è che le amministrazioni locali distribuiscano credenziali convenzionali imputabili. Infatti per non creare discriminazioni devono consentire l'accesso ai servizi che richiedono l'accertamento della identità a tutti, anche a coloro che non dispongono di una Carta d'Identità Elettronica o di una Carta Nazionale Servizi o che non sono in condizione di usarla, essendo privi di una stazione di lavoro attrezzata.

Tra le modalità di registrazione discusse in precedenza, la più semplice per gli utenti e la meno costosa per gli Enti locali è sicuramente la **registrazione telematica diretta** sul sito dell'Ente da parte di soggetti in grado di identificarsi con certezza utilizzando **altre credenziali imputabili** valide, o comunque accettate dall'ente. In questa ipotesi sarà possibile comunicare all'utente le credenziali dell'ente **direttamente durante la procedura informatica di registrazione** e risparmiare i costi di provisioning connessi alle altre modalità di registrazione.

Tuttavia chi non dispone già di credenziali imputabili, come ad esempio una CIE, una CNS o anche una di Carta di Firma Digitale (CFD), oppure della concreta possibilità di usarle sulle proprie stazioni di lavoro connesse in internet - e si tratterà in pratica della **quasi totalità degli utenti** - non sarà neppure in grado di registrarsi direttamente per via telematica e l'amministrazione dovrà ricorrere o al riconoscimento a vista, con consegna sicura al titolare della parte segreta delle credenziali, che tipicamente viene consegnata in busta cieca, oppure dovrà ricorrere alla onerosa gestione delle richieste di registrazione inviate via fax o per lettera, accompagnate dalla fotocopia del documento d'identità e del tesserino fiscale. (Quest'ultima modalità è stata ad esempio adottata per la registrazione al portale del Comune di Roma).

Si tratta in ogni caso di modalità di registrazione che comportano **per i cittadini adempimenti fastidiosi e poco graditi**, che li disincentivano dall'uso dei servizi in rete. Si tratta anche di modalità costose per l'Ente locale, infatti la gestione delle necessarie procedure organizzative per l'attribuzione di credenziali imputabili comporta **extra costi** elevati e spesso insostenibili[7]. Per questo motivo numerose amministrazioni, con scarsa sensibilità per la sicurezza e per la tutela della privacy degli utenti, continuano a rilasciare

[7] *Si tratta di costi di difficile valutazione, ma probabilmente dell'ordine dei 3 € per abitante di comuni medio grandi.*

credenziali non imputabili (sicuramente meno costose) anche per accedere a servizi che richiederebbero l'accertamento dell'identità.

La possibilità di **allargare il bacino degli utenti** che possono accedere alla registrazione telematica diretta, includendo anche chi non è in grado di usare una smart card pur disponendone, si potrebbe concretizzare se gli Enti locali accettassero per la registrazione ai propri siti, oltre alla CIE o alla CNS o anche alla carta di firma digitale, anche l'uso delle **credenziali fiscali** dell'utente (UserID = Codice Fiscale, Password e PIN associati al Codice Fiscale) che l'Agenzia delle entrate fornisce a tutti i soggetti censiti nell'Anagrafe tributaria (quindi a tutti i soggetti che hanno titolo ad ottenere servizi delle pubbliche amministrazioni).

In questo modo si ottiene un duplice vantaggio: gli Enti locali potranno **risparmiare integralmente i costi di provisioning** della registrazione a vista o via fax per i cittadini che sono già registrati presso l'Agenzia delle entrate e i cittadini, dopo essersi registrati presso l'Agenzia delle entrate, potranno registrarsi al sito di qualsiasi ente con una procedura semplice ed immediata.

È verificato che, allo stato dell'arte della tecnologia internet già in uso presso le amministrazioni, realizzare questa possibilità è estremamente semplice e soprattutto ha un costo marginale praticamente nullo rispetto ai costi che ogni Ente locale dovrebbe comunque affrontare per adeguarsi alla normativa vigente.

Per rendere possibile questa soluzione, l'Agenzia delle entrate dovrà realizzare un **Servizio di certificazione delle credenziali fiscali** accessibile agli enti interessati. Il cittadino che intende usare le proprie credenziali fiscali per registrarsi al sito di un ente, verrà automaticamente ridiretto verso il Servizio di certificazione della Agenzia delle entrate, con modalità tecniche che assicurano che la componente segreta delle sue credenziali fiscali non venga in alcun modo resa nota al sistema informativo dell'ente. Dopo aver verificato le credenziali il Servizio di certificazione restituirà il controllo dell'interazione al sito dell'ente, inviandogli una **asserzione di identità** basata sul codice fiscale. La registrazione può essere così completata comunicando direttamente all'utente, della cui identità si ora ha certezza, le nuove credenziali imputabili necessarie per l'accesso ai servizi dell'Ente locale. (Senza entrare qui in aspetti di natura tecnica, si tratta di gestire interazioni tra sistemi informatici tipiche del mondo internet ed integralmente basate su protocolli standard adottati a livello internazionale).

Il servizio erogato dalla Agenzia delle entrate equivale a certificare la qualità di soggetto registrato presso l'amministrazione finanziaria dell'utente e alla verifica del suo codice

fiscale e dovrebbe rientrare nelle previsioni del comma 3, Art. 43 del DPR n. 445, 28 dicembre 2000[8] e dell'Art. 50 del Codice della amministrazione digitale.

Per realizzare questa soluzione si rende necessario un intervento tecnico sui portali degli Enti locali di tipo non invasivo e di modesta entità, infatti per conformità alla normativa vigente questi dovrebbero essere già oggi predisposti per la gestione di ogni altro strumento imputabile previsto dalla legge, in particolare di CIE o CNS.

Nell'ipotesi che gli Enti locali possano fruire di un Servizio di asserzione dell'identità basato sulle credenziali fiscali è logico domandarsi perché limitare questo accesso alla sola esigenza di registrazione e non utilizzare le stesse credenziali anche per l'autenticazione all'accesso ai servizi, in luogo delle credenziali proprie emesse dall'ente. In questo caso gli Enti locali potrebbero evitare non solo i costi di provisioning, ma anche i costi di gestione di un proprio servizio di autenticazione.

Senza entrare in considerazioni di opportunità politica, dal punto di vista tecnico una evoluzione in questa direzione non appare auspicabile, per le seguenti ragioni:

- Il funzionamento dei sistemi informativi degli Enti locali verrebbe permanentemente a dipendere da un servizio erogato della Agenzia delle entrate; quindi non solo al momento della registrazione degli utenti, quindi in un numero circoscritto di casi, ma per ogni volta che un utente accede ad un qualsiasi servizio dell'Ente, con evidenti criticità sulla **disponibilità** dei servizi.
- Il Servizio di certificazione dell'Agenzia delle entrate verrebbe coinvolto ad ogni accesso a servizi in rete fatto da ogni utente nel paese, con implicazioni sia per il dimensionamento prestazionale del servizio, sia per la sicurezza in relazione alle esigenze di tutela della privacy.

D'altronde, e come si è già argomentato, l'adozione generalizzata delle credenziali fiscali non è la sola possibilità per dotare gli utenti credenziali convenzionali uniche.

Numerosi Enti locali segnalano da tempo l'esigenza di risolvere con un approccio condiviso e modalità uniformi il problema della gestione dell'identità degli utenti dei propri servizi in rete e potranno trovare in questa proposta una soluzione capace di eliminare i rilevanti extra costi causati della mancata disponibilità e fruibilità di CIE o CNS, proprio nel

[8] *DPR 445, 28 dicembre 2000 Art. 43, comma 4: "Al fine di agevolare l'acquisizione d'ufficio di informazioni e dati relativi a stati, qualità personali e fatti, contenuti in albi, elenchi o pubblici registri, le amministrazioni certificanti sono tenute a consentire alle amministrazioni procedenti, senza oneri, la consultazione per via telematica dei loro archivi informatici, nel rispetto della riservatezza dei dati personali. (R)*

momento in cui sono pronti ad erogare i propri servizi in rete e soprattutto potranno rendere possibile l'accesso a tutti i cittadini.

6 Le modifiche normative necessarie

L'effetto combinato dei commi 1 e 3 dell'Art. 64 "*Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni"* del DLgs. 7 marzo 2005, n. 82, Codice della amministrazione digitale, impone a partire dal 31 dicembre 2007 che la Carta d'Identità Elettronica (e la CNS) sia **l'unico tipo di credenziale utilizzabile** per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni che **richiedono l'autenticazione informatica**. Fino a quella data il comma 2, dell'Art. 64 consente alle amministrazioni di adottare anche altri tipi di credenziali, purché **consentano di accertare l'identità di chi richiede l'accesso.**

Così come è formulato il Codice della amministrazione digitale richiede **sempre l'uso di credenziali imputabili per accedere a qualsiasi servizio**: infatti CIE e CNS sono imputabili per definizione, mentre il comma 2 esplicitamente lo richiede per gli altri tipi di credenziali. La finalità dell'Art. 64 dovrebbe invece essere solo quella di stabilire il principio che l'accesso a **servizi dovuti alla persona,** o che implicano **accesso a dati personali o sensibili,** possa essere **consentito solo a che ne ha diritto**, senza necessariamente individuare le modalità e le tecnologie di attuazione, che dovrebbero essere più opportunamente demandate alle Regole tecniche di cui all'Art. 71 del Codice stesso, anche per ragioni di flessibilità in considerazione delle evoluzioni tecnologiche possibili nel campo della identificazione.

Si è già ampiamente argomentato che la formulazione dell'Art. 64, che intende l'autenticazione informatica come mezzo per accertare l'identità dell'utente, è priva di fondamento: **i servizi non possono essere suddivisi in quelli che richiedono l'autenticazione informatica oppure in quelli che non la richiedono, ma in quelli che richiedono o meno l'accertamento dell'identità**. L'autenticazione infatti è funzione sempre necessaria per l'accesso non anonimo ad un sistema informatico, indipendentemente dal fatto che le credenziali presentate siano state attribuite a seguito dell'accertamento dell'identità dell'utente. La norma così formulata produce effetti pratici indesiderabili e paradossali perché esistono sicuramente servizi erogati delle pubbliche amministrazioni che, per ragioni tecniche e organizzative del servizio, richiedono l'autenticazione dell'utente, senza tuttavia la

necessità di accertarne l'identità personale. Per questi servizi non si dovrebbe imporre l'uso di credenziali imputabili[9] tanto più se si tratta di una smart card.

Imporre, sempre e comunque, l'uso di credenziali imputabili e, dopo il 31 dicembre, della sola CIE (o della CNS), **indipendentemente dalla tipologia del servizio richiesto**, non appare razionale e sostenibile in pratica. Si ritorna al tema fondamentale, finora eluso, della **classificazione dei servizi in base alle esigenze di sicurezza e di accertamento dell'identità**.

Esiste anche una esigenza di **coerenza generale tra norme vigenti attualmente in contrasto tra loro**, in particolare tra quelle che regolano gli strumenti di autenticazione previsti per i **cittadini in qualità di utenti** dei servizi delle pubbliche amministrazioni (per i quali si richiede a regime l'uso della CIE) e quelle del DLgs. 30 giugno 2003, n. 196 "***Testo Unico sulla tutela della privacy***" che regolano gli strumenti di autenticazione previsti per gli **addetti al trattamento di dati personali o sensibili** di soggetti terzi, per i quali sono considerate sufficienti credenziali di tipo convenzionale.

Fintanto che l'Art. 64 resta in vigore, sarà ovviamente necessario che le amministrazioni ottemperino integralmente alle sue prescrizioni, indipendentemente dalle difficoltà o impossibilità di acceso ai servizi che ne deriveranno ai cittadini, ma è sicuramente auspicabile che **il legislatore adotti rapidamente una nuova formulazione**, che risponda meglio alle esigenze di sicurezza e di praticabilità, che è doveroso garantire.

La formulazione attuale dell'Art. 64 è riportata nel seguito

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

> *1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono* **strumenti** *per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni* **per i quali sia necessaria l'autenticazione informatica**.
>
> *2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati* **che richiedono l'autenticazione informatica anche con strumenti** *diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque*

[9] *Si è già osservato che poiché per esigenze gestionali non si può escludere che ci si debba autenticare per prenotare via Internet un campo da tennis comunale sembra paradossale imporre per questo servizio l'uso della CIE.*

consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è **fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. E' prorogato alla medesima data** *il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.*

La formulazione suggerita potrebbe essere la seguente:

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono ***strumenti di autenticazione informatica*** *per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni.*

2. ***Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali****, le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati* ***che, in base alle regole tecniche di cui all'art. 71 e nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente, richiedono l'identificazione personale dell'utente, anche con strumenti di autenticazione informatica*** *diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.*

3. Con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è ***prorogato a data comunque non successiva al 31 dicembre 2007,*** *il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.*

Nella formulazione proposta il comma 2 rinvia alle Regole tecniche la **definizione dei criteri di classificazione dei servizi** in base ai requisiti minimi di imputabilità e di sicurezza degli strumenti da utilizzare per l'autenticazione informatica all'accesso. In questo modo si mantiene anche la necessaria apertura all'introduzione di tecnologie di identificazione innovative basate, ad esempio, sulle caratteristiche biometriche.

Le Regole tecniche in materia di sicurezza all'accesso potrebbero costituire un necessario e dovuto riferimento per le amministrazioni, soprattutto per gli Enti locali, per metterli nelle condizioni di realizzare modalità di accesso ai propri servizi uniformi su tutto il territorio nazionale, evitando il rischio insito nelle norme vigenti, ed evidenziato anche nel Programma dell'Unione, di creare una giungla degli strumenti di autenticazione informatica.

In coerenza con le modifiche proposte all'Art. 64 è necessario modificare anche l'Art. 65 che riguarda la **presentazione di istanze e dichiarazioni per via telematica alla pubblica amministrazione** e porre rimedio all'altra incongruenza normativa già segnalata. Infatti per quanto riguarda la CIE e la CNS i due articoli appaiono incoerenti tra loro, perché mentre l'Art. 64 impone l'uso della CIE o CNS per qualsiasi servizio, l'Art. 65, comma 1, lettera b consente ad ogni amministrazione di limitarne l'uso nel caso di presentazione di istanze:

Art. 65. Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;

b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, **nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente***;*

c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, **nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente** *e fermo restando il disposto dell'articolo 64, comma 3.*

2. Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento; **resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione mediante la firma digitale**.

L'attuale formulazione dell'Art. 65 determina, soprattutto per le istanze da presentare agli Enti locali, una situazione paradossale e potenzialmente caotica: qualora infatti ogni amministrazione stabilisse per gli stessi servizi regole diverse per l'uso della CIE/CNS sarebbe impossibile assicurare ai cittadini l'omogeneità nel paese dei livelli essenziali delle prestazioni.

La nuova formulazione dell'Art. 65 dovrà essere coerente con la riformulazione dell'Art. 64 e soprattutto assicurare in ogni caso almeno la possibilità di una **sottoscrizione elettronica dell'istanza** nelle varie forme previste, che è altra cosa rispetto alla esigenza di **autenticazione dell'utente**. Per approfondire questa ulteriore materia si rimanda ad un precedente documento dell'autore, che illustra le proposte di integrazioni al Codice in materia di firme elettroniche[10].

[10] *Alessandro Osnaghi, Firme elettroniche e documento informatico: il Codice richiede ulteriori integrazioni. Pubblicato in "ASTRID - Rassegna n. 30 2006.*